SHORT PROJECT

PHAZE FOUR

HAFIZ NAVEED UDDIN KAIRIZ CYBER TECHNOLOGIES

Phase 4: Monitoring and Incident Response Report

Objective: To establish effective monitoring capabilities and incident response procedures to enhance the overall security posture of the network.

Tools Used:

- SIEM System: Splunk Enterprise
- Alerts Configuration: SIEM rules for detecting suspicious activities
- Incident Response Plan (IRP): Developed based on industry best practices

Activities Performed:

1. **SIEM System Setup:**
    - Installed and configured Splunk Enterprise as the SIEM solution.
    - Integrated with existing network infrastructure to monitor network traffic and security events.
2. **Alerts Configuration:**
    - Configured SIEM rules to detect potential security incidents such as:
        - Anomalies in network traffic patterns.
        - Unauthorized access attempts.
        - Malware infections and suspicious file transfers.
3. **Incident Response Plan Development:**
    - Developed a comprehensive Incident Response Plan (IRP) outlining:
        - Roles and responsibilities of incident response team members.
        - Procedures for identifying, containing, and mitigating security incidents.
        - Communication protocols during incident response activities.
4. **Regular Drills and Tabletop Exercises:**
    - Conducted regular tabletop exercises to simulate various security incidents.
    - Tested the effectiveness of the IRP and the response capabilities of the incident response team.
5. **Comprehensive Final Report Compilation:**
    - Documented all activities conducted during Phase 4, including:
        - Details of SIEM setup and configuration.
        - Results and outcomes of alert configurations and incident response drills.
        - Summary of findings and recommendations for ongoing security improvements.
6. **Presentation to Stakeholders:**
    - Prepared a presentation summarizing the Phase 4 activities:
        - Highlighted key findings from monitoring and incident response efforts.
        - Discussed actions taken to enhance network security and mitigate potential threats.
        - Presented recommendations for continuous improvement and future security measures.

Recommendations:

- Implement continuous monitoring and periodic reviews of SIEM rules and alert configurations.
- Conduct regular training sessions for incident response team members to ensure readiness during real-world incidents.
- Enhance collaboration between IT security teams and other departments to strengthen overall security awareness and response capabilities.

Conclusion: Phase 4 has significantly improved the network's security posture by implementing robust monitoring capabilities and establishing effective incident response procedures. The proactive measures taken will help mitigate potential security risks and enhance overall resilience against cyber threats.